SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

ZAVRŠNI RAD

SIGURNOSNI ASPEKT RAČUNOVODSTVA U E-OBLAKU

Mentor:
prof. dr. sc. Željko Garača

Student:
Hrvoje Maletić

Split, rujan 2018.

SADRŽAJ:

1. UVOD 4

2. OSNOVE RAČUNOVODSTVENIH SUSTAVA U E-OBLAKU 6

2.1. Računovodstveni informacijski sustavi 6

2.2. Razvoj računovodstva 7

2.3. Računovodstvo u oblaku 9

2.3.1. Prednosti 9

2.3.2. Nedostatci 10

2.3.3. Primjer Republike Hrvatske 10

3. SIGURNOSNI ASPEKTI 12

3.1. Sigurnosna politika 13

3.2. Procjena i umanjivanje sigurnosnog rizika 13

4. SIGURNOSNE PRIJETNJE 17

4.1. Ciljane prijetnje 17

4.1.1. Povreda podataka 17

4.1.2. Nedostatan identitet, vjerodostojnost i upravljanje pristupom 18

4.1.3. Nesigurna sučelja i API-ji 18

4.1.4. Gubitak podataka 18

4.1.5. Ranjivost sustava 19

4.1.6. Otmica računa 19

4.1.7. Nedovoljna pažnja 19

4.1.8. Zlouporaba i neželjena upotreba oblak usluga 19

4.1.9. Uskraćivanje usluge 20

5. METODE ZAŠTITE 21

5.1. Organizacijske mjere 21

5.2. Fizičke mjere 23

5.3. Programske mjere 24

5.4. Primjeri metoda zaštite na ciljane prijetnje 25

5.4.1. Nedostatan identitet, vjerodostojnost i upravljanje pristupom 25

5.4.2. Nesigurna sučelja i API-ji 25

5.4.3. Gubitak podataka 26

5.4.4. Otmica računa 26

5.4.5. Zloupotreba i neželjena upotreba oblak usluga 26

6. ZAKLJUČAK 27

LITERATURA 28

PRILOZI 29

SAŽETAK 30

SUMMARY 31

1. UVOD

Dva temeljna resursa za uspješno poslovanje su znanje i informacije, a svi ostali resursi postali su ovisni o navedenima iako oni nemaju definiranu financijsku vrijednost. Uvjetovane vremenom i mjestom informacije dobivaju na vrijednosti, a time se povećava i efikasnost i efektivnost rada određene poslovne organizacije.

Kroz vrijeme, podaci su se prikupljali, pohranjivali, analizirali i distribuirali na različite načine. Tako nastali informacijski sustavi razvijali su se i dalje se razvijaju, a danas predstavljaju nužnost na globalnoj razini. I iako, kako je navedeno na početku uvoda, informacije nemaju definiranu financijsku vrijednost, informacijski sustavi predstavljaju investiciju jer se njima tvrtke koriste radi ostvarivanja profita.

U svakoj poslovnoj organizaciji događaju se financijske aktivnosti i transakcije, a bilježenjem istih bavi se računovodstvo. Učinkovito poslovanje određeno je funkcijom računovodstva čije informacije omogućavaju kontrolu, a samim time i planiranje namijenjeno poslovnom subjektu i eksternim korisnicima.

Pozitivni pomak dogodio se osuvremenjenjem računovodstvenih informacijskih sustava koji su se usko povezali s informacijskim tehnologijama koje su danas norme poslovanja. Suvremeni računovodstveni informacijski sustavi uključuju ne samo financijske, već i nefinancijske podatke koji se pohranjuju na Internet umjesto na računalo i time se uvodi informatički koncept računalstva u oblaku (eng. *cloud*). „Danas se pojam *cloud* izjednačava s dostupnošću, lakoćom i brzinom upravljanja podacima."[1] Oblak je omogućio korisnicima (računovođama) dohvaćanje podataka s bilo kojeg mjesta i u bilo koje vrijeme.

Informacijska tehnologija je podrška izgradnji integralnog informacijskog sustava koji jedini može osigurati kvalitetnu složenost informacija zadovoljavajuće brzine. Organizacija svih relevantnih podataka, metoda i postupaka omogućuje racionalnije korištenje radnoga vremena, povećanje pouzdanosti sustava i smanjenje troškova poslovanja brisanjem granica između funkcija unutar poslovnog subjekta kojim onemogućuje dvostruki unos istih podataka. Primjenom računalne opreme upravo to predstavlja integrirani informacijski sustav poslovnog subjekta.

Negativni aspekt novijih oblika računovodstvenih sustava koji su internetski povezani je rizik i pitanje sigurnosti i dostupnosti informacija i podataka te sama internetska povezanost na određenoj lokaciji.

[1] Lukić, K. (2016.): Računovodstvo u oblaku u Republici Hrvatskoj, Finiz, str. 262.

Problem sigurnosti u obavljanju računovodstvenih operacija u poslovno informacijskom sustavu tema je kojom će se baviti ovaj rad.

Ciljevi rada su istražiti probleme sigurnosti i istražiti metode zaštite podataka u računovodstvu u e-oblaku.

Metode kojima će se koristiti u ovom radu su metoda deskripcije, metoda sinteze i analize, i metoda komparacije. Korištene kroz cijeli rad, ove metode prikladne su za predmetno istraživanje jer istovremeno omogućavaju naznačivanje obrađene literature i kritički stav prema ključnim pitanjima teme.

Prvi dio rada obuhvatit će osnovne definicije i uopće koncept računovodstvenih sustava u e-oblaku. Nakon kratkog osvrta na razvoj i podjelu računovodstva, navest će se prednosti i nedostatci računovodstvenih sustava u e-oblaku te će se navesti način korištenja istih u Republici Hrvatskoj.
U drugoj cjelini bit će opisani sigurnosni aspekti računovodstva u oblaku odnosno sigurnosni aspekti samoga oblaka, nadalje, bit će definirana sigurnosna politika te rizici i procjena i umanjivanje istih.
U trećem dijelu analizirat će se prijetnje koje se događaju oblaku, a načini zaštite od istih zaključit će ovaj rad.

2. OSNOVE RAČUNOVODSTVENIH SUSTAVA U E-OBLAKU

Definicija računovodstva koja se najčešće upotrebljava jest ona „Američkog instituta ovlaštenih javnih računovođa (*American Institute of Cerified Public Accountants* - AICPA), koja kaže da je računovodstvo „vještina bilježenja, razvrstavanja, skraćenog prikazivanja i interpretiranja u novčanom obliku izraženih poslovnih događaja koji su bar djelomično financijske naravi i interpretiranje iz toga proizašlih podataka.“[2] Također možemo reći i da je računovodstvo sistem evidencije koji na poseban i strogim pravilima reguliran način evidentira, kontrolira i analizira kretanje sredstava u poslovnim poduzećima.

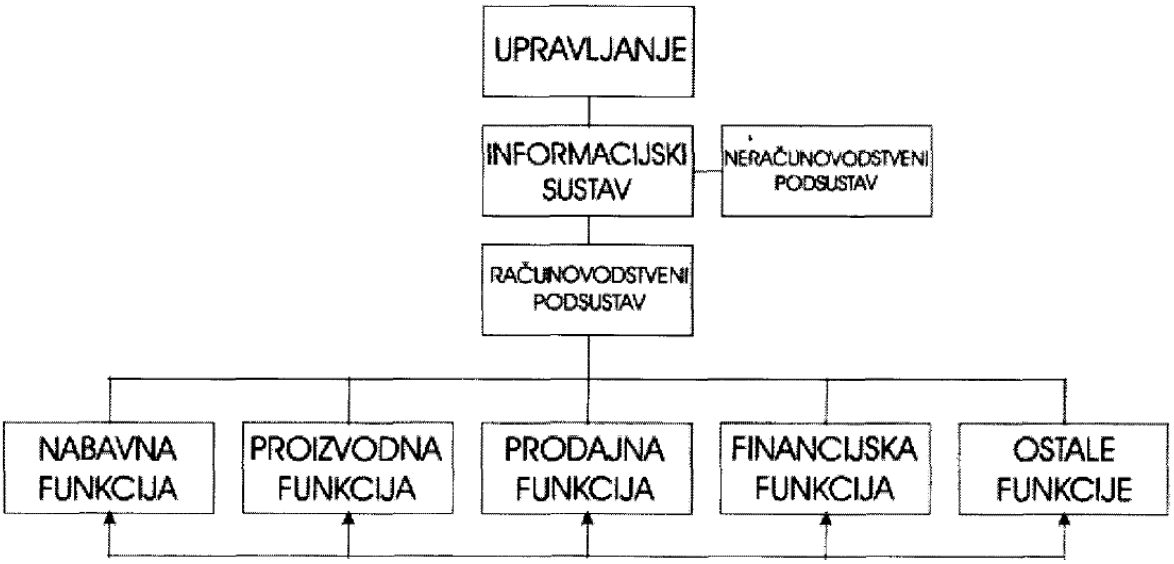
2.1. Računovodstveni informacijski sustavi

Pojam računovodstvenog informacijskog sustava (RIS) označava podsustav ukupnog informacijskog sustava koji je temeljni izvor informacija o poslovanju poduzeća. RIS je skup medusobno povezanih elemenata koji različite poslovne transakcije pretvaraju u računovodstvene informacije te je uvijek naglasak na kvantitativnim informacijama.

Po J.K.Wilkinsonu RIS se sastoji od 5 modula:
1. podsustav prihoda
2. podsustav rashoda
3. podsustav upravljanja resursima
4. podsustav glavne knjige i financijskog izvještavanja
5. proizvodno-konverzijski sustav

Forma u kojoj se podaci prezentiraju su financijska izvješća i ona su alat za daljnje poslovno odlučivanje. Upravljački podsustav odnosno menadžment svakoga poslovnog subjekta koristi te informacije za donošenje različitih poslovnih odluka.

[2] Crnković, L., Hadrović Zekić, B., Mijoč, I. (2006.): Povijesni razvoj računovodstvenog informacijskog sustava – od glinene pločice do računala, Ekonomski vjesnik br. 1 i 2 (19), str. 65 - 78



Slika 1: Povezanost računovodstvenog podsustava i upravljanja

Izvor: Marković, B., opt. cit., str. 10.

2.2. Razvoj računovodstva

Najstariji dokazi korištenja računovodstva dolaze iz 7500. godine prije Krista te su pronađeni u Jerihonu i pokazuju bilježenje stanja zaliha stoke i žita. Egipćani su počeli razvijati državno knjigovodstvo, odnosno na razini države prvi su razvili evidenciju stanja žita vođenu na papirusu.

Najstarije nađene bilješke dvostavnog knjigovodstva (koje za razliku od prethodnih sustava vođenja knjiga koji su vodili transakcije na jedan konto bilježi svaku transakciju na najmanje dva različita konta glavne knjige računa) su Genovske tvrtke Giovanni Farolfi & Co. iz 1340. godine.

Prema A. C. Littletonu sljedećih sedam uvjeta je potrebno za postojanje „pravog“ dvostavnog knjigovodstva:

1. Privatno vlasništvo - snaga promjene vlasništva, knjigovodstvo je bilo okrenuto vođenju bilježaka o vlasništvu i vlasničkim pravima
2. Kapital - uključivanje bogatstva u proizvodnju; u suprotnom bi trgovina bila trivijalna i potraživanje ne bi postojalo
3. Trgovina - širom rasprostranjena razmjena dobara; zbog čistog lokalnog trgovanja na male količine nije bilo moguće stvoriti pritisak na poslovanje koje bi poticalo na razvoj organizacijskih sustava mijenjajući postojeću zbrku u vođenju evidencije

4. Potraživanje - trenutno korištenje budućih dobara
5. Pismo (pisanje) - mehanizam za vođenje trajnih bilješki u uobičajenom jeziku, zbog ograničenog ljudskog pamćenja
6. Novac - sredstvo razmjene, nema potrebe za knjigovodstvenim transakcijama osim ako se time smanjuju transakcije određene novčanim vrijednostima
7. Zbrajanje - sredstvo izračunavanja monetarnih detalja dogovora

Prve upute o upotrebi dvostavnoga knjigovodstva napisao je 1458. godine Benedikt Kotruljević u knjizi "O trgovini i savršenom trgovcu"13, gdje je iznio značaj dvostavnoga knjigovodstva za trgovce.

Tijekom 1940-ih započeo je razvoj prve generacije računala koja su koristila vakuumske cijevi s elementarnim programskim mogućnostima (UNIVAC). Druga generacija računala, razvijena 1950tih, koristila je poluvodiče odnosno tranzistore s razvijenim naprednim programskim mogućnostima. U ovo doba IBM (*International Business Machines*) počinje razvoj poslovnih računala da bi se 1953. na tržištu pojavio IBM 702 koji je prilagođen upotrebi u računovodstvu, a iste godine je Arthur Andersen kompjutorizirao obračun plaća za General Electric. Upotreba računala se globalizira, a ostale revizorske tvrtke ("Big 8") počele su koristiti računala u konzultantske svrhe. Elektronske komponente korištene u četiri generacije računala. Treća generacija računala, koja se proizvodila 1960-ih koristila je integrirane tranzistorske krugove i viši nivo programskih jezika. Četvrtu generaciju računala, razvijenih tijekom 1970-ih, karakterizirao je vrlo velik nivo integriranih čipova s programskim jezicima na višoj razini i pojava prvih osobnih računala - Apple II, a tri godine kasnije na istom računalu kreiran je prvi tablični kalkulator VisiCals za Apple II. Peta računalna generacija, karakteristična za početak 1980-te, imala je još manje integrirane čipove, a programski jezici su na sve višoj razini, tako da su računala postajala sve brža, pouzdanija, jeftinija i lakša za korištenje. Napredak u računalnoj tehnologiji virtualno je dostigao svoj eksplozivni nivo tijekom 1980-ih s pojavom stolnih računala, velikim primamim i sekundarnim memorijama, kao još uvijek rastućom upotrebom elektronske pošte, Interneta, intraneta i međupovezivanja.

S navedenim razvojem tehnologije dolazi do podjele računovodstva na tradicionalno i računovodstvo u oblaku. Tradicionalno računovodstvo koristi tradicionalni računovodstveni softver, pod kojim se podrazumijeva softver koji je instaliran na računalu nekog poslovnog subjekta koji ga koristi za vođenje poslovnih knjiga i ostalih administrativnih poslova.

2.3. Računovodstvo u oblaku

Računovodstvo u oblaku je računovodstvo kod kojeg se računovodstveni softver, kao i podaci nalaze na udaljenom serveru koji nije u vlasništvu određenog poslovnog subjekta. Definicija Nacionalnog instituta za standarde i tehnologiju SAD-a (Mell & Grance, 2011) opisuje oblak kao model koji omogućuje pogodan pristup "po zahtjevu" mreži zajedničke grupe podesivih računalnih resursa (npr. mreža, servera, skladištenja, aplikacija i usluga) koji se korisniku mogu dostaviti brzo uz minimalan napor upravljanja ili interakcije s davateljem usluge. Oblak predstavljaju računalni resursi, računalna oprema i internetska povezanost koja omogućuje ostale procese.
Ključna razlika tradicionalnog računovodstva i računovodstva u oblaku je internetska povezanost. Razlike se također nalaze u vlasništvu licence softvera koja je kod tradicionalnog računovodstva u rukama vlasnika, a kod računovodstva u oblaku ona je samo u najmu. Također kod tradicionalnog računovodstva su hardver,Windows i SQL server priskrbljeni od strane poslovnog subjekta dok su kod računovodstva oni uključeni u najam. Kod tradicionalnog računovodstva, kako bi tvrtka pristupila podacima, neophodna je internet veza u svakom trenutku, kao i neprekidan rad servera na kojima se podaci nalaze. Kod računovodstva u oblaku podacima se može pristupiti u bilo koje vrijeme i to s bilo kojim elektronskim uređajem koji koristi neki od web pretraživača.

2.3.1. Prednosti

„Glavne prednosti računovodstva u oblaku su niži troškovi ulaganja i održavanja, pristupačnost i fleksibilnost sustava, brzina i način obrade podataka, usklađenost sustava, jednostavnost i efikasnost, smanjenje rizika od uništenja podataka i općenita sigurnost sustava."[3] Oblak omogućava računovođama pristup i rad na podacima u bilo koje vrijeme s bilo kojeg mjesta. Kada govorimo o sigurnosti većina poslužitelja aplikacija u oblaku nudi visoku razinu sigurnosti te puno veću razinu od one kod lokalnih servera. Računovodstvo u oblaku se automatski prilagođava računovodstvenim standardima te ima ugrađene module za internu kontrolu.

[3] Lukić, K. (2016.): Računovodstvo u oblaku u Republici Hrvatskoj, Finiz, str. 262.

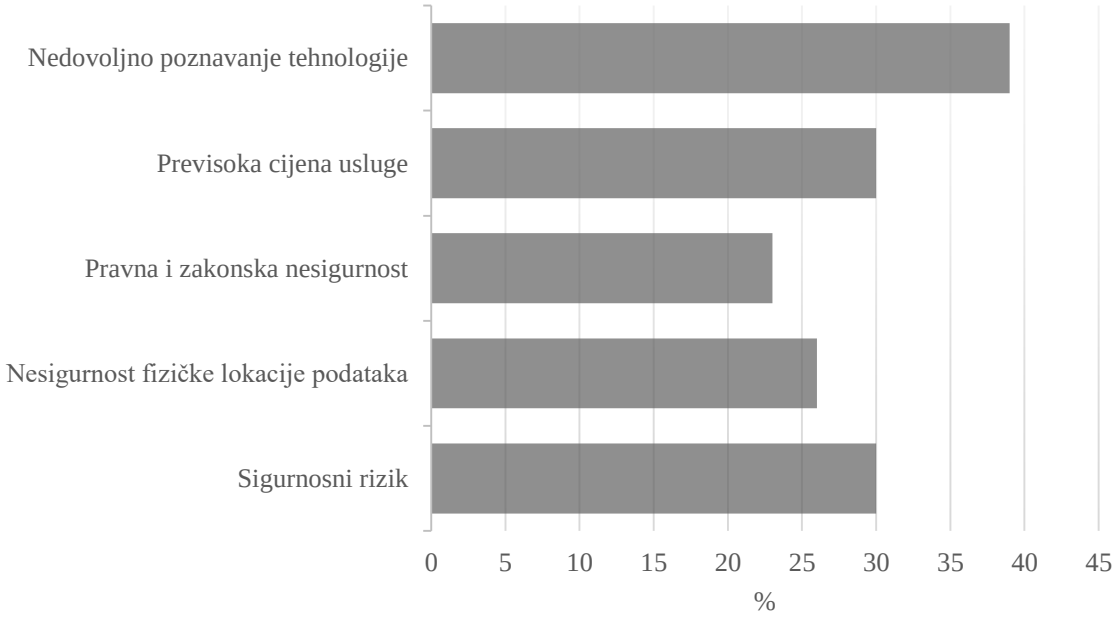
2.3.2. Nedostatci

Nedostatci računovodstva u oblaku najčešće su povezani uz sigurnosne rizike koji su uvijek prisutni. Povjerljive informacije pružene davatelju usluga mogu zadati velike probleme poslovnom subjektu. Za računovodstvo u oblaku neophodna je jaka internetska povezanost. Također u slučaju zakazivanja programa na oblaku, klijentu nije omogućen pristup ili prilika otklanjanja problema na oblaku. Savić i Janković (2015.) opažaju da su nedovoljna kvaliteta komunikacijske infrastrukture, komplikacije zakonske regulative te nepovjerenje i neinformiranost gospodarskih subjekata, jedni od glavnih razloga nedovoljne primjene cloud computing tehnologije.

2.3.3. Primjer Republike Hrvatske

Na primjeru Republike Hrvatske može se ocijeniti nedovoljno povjerenje i općenito neznanje računovođa o pojmovima kao što su oblak i računovodstvo u oblaku. Nedovoljna informiranost o računovodstvu u oblaku je najveća prepreka ka široj upotrebi. Za analizu upotrebe računovodstva u oblaku u Republici Hrvatskoj koristit će se istraživanje Karla Lukića iz 2016. godine. Prvo pitanje u anketi se odnosilo na upoznatost računovođa s konceptom računalstva u oblaku. Najveći broj ispitanika (23) odgovorilo je da dobro (3) i vrlo dobro upoznato (4) konceptom clouda. Dobru upoznatost slijedi potpuna upoznatost (5) 16 ispitanika te neupoznatost (0) od strane 14 ispitanika, dok je 13 ispitanika dovoljno upoznato (2) konceptom računalstva u oblaku. Najmanji broj ispitanika (11) nedovoljno je upoznato (1) konceptom clouda. Prosječni odgovor na 1. anketirano pitanje pritom je 2.78, pri čemu je sigurno zaključiti da je na prostoru Republike Hrvatske informiranost o računalstvu u oblaku dovoljno dobra. Drugo pitanje online ankete kao cilj imalo je pružiti točan i precizan pogled na informiranost trenutnih i budućih računovođa o računovodstvu u oblaku. Pritom je 31 ispitanik potpuno neupoznat (0) konceptom cloud računovodstva, kojega slijedi djelomična ili dobra upoznatost (3) 25 ispitanika. Najmanji broj ispitanika (7) potpuno je upoznat (5) konceptom računovodstva u oblaku dok je prosječni odgovor svih ispitanika iznosio 1.95, što se može protumačiti kao dovoljna upoznatost spajanja koncepata oblaka i računovodstva. U skladu s rezultatima prvog anketiranog pitanja o upoznatosti cloud tehnologije općenito, pri čemu je većina ispitanika potvrdno odgovorila da je dobro upoznata s općenitom tehnlogijom rješenja u oblaku, većina trenutnih i budućih računovođa unutar Republike Hrvatske nije

dobro upoznata konceptom računovodstva u oblaku. Posljednje anketirano pitanje pružilo je odgovor na način kako ispitanici doživljavaju oblak po pitanjima sigurnosti i rizika. Većina ispitanika (44%) nikada ne bi povjerila svoje poslovne podatke trećim osobama na serveru za koji ne zna gdje se točno nalazi, dok bi manji postotak od 26% to bio spreman učiniti, no veći dio ispitanika (30%) ostaje skeptičan i neodlučan pri povjerenju podataka ponuđačima cloud usluga. Nizak postotak povjerenja u cloud accounting na području Republike Hrvatske razumljiv je ako se uzmu u obzir rezultati prethodnih pitanja o neinformiranosti budućih i trenutnih računovođa o cloudu i računovodstvu u oblaku, stoga je za pretpostaviti da će ispitanici biti skeptični prema tehnologiji koju u potpunosti ne razumiju.



Grafikon 1: Zapreke u korištenju koncepta računalskog oblaka u Republici Hrvatskoj
Izvor: Državni zavod za statistiku

Kao moguća rješenja navedenih poteškoća, preporučuju se dodatne edukacije i obrazovanje o uslugama računovodstva u oblaku i općenitog načina na koji cloud accounting funkcionira i poboljšava poslovanje gospodarskog subjekta. Navedene mjere povećale bi sigurnost o načinima rada i vrstama usluga računovodstva u oblaku, pri čemu bi se povjerenje u ponuđače tih usluga zasigurno povisilo.

3. SIGURNOSNI ASPEKTI

Sigurnost i zaštita financijskih podataka oduvijek je u fokusu poslovnog subjekta, bez obzira koji softver koristi za izvršavanje operativnih aktivnosti u računovodstvu i financijskom upravljanju. Svaki poslovni subjekt prije nego se opredijeli za primjenu računovodstva u oblaku želi znati da su financijski podaci adekvatno zaštićeni i dostupni, u skladu sa dodijeljenim ovlastima. Potrebno je poštovati:

1. Privatnost podataka
2. Zaštitu od neovlaštenog pristupa
3. Integritet podataka
4. Dostupnost
5. Brz pristup podacima
6. Ugovorni odnos koji će zakonski regulirati prava i obveze i korisnika i pružatelja usluga

Tablica 1: Uobičajeni zahtjevi sigurnosti

CILJ	OPIS
Povjerljivost	Osiguravanje da se informacije ne otkriju ljudima koji nemaju prava pristupa.
Integritet	Osiguravanje da je informacija koja se čuva na sustavu prava reprezentacija informacije koja se trebala čuvati na poslužitelju i da nije modificirana od strane neovlaštene osobe.
Dostupnost	Osiguravanje da resursi za obradu informacije nisu nedostupni zbog ujtecaja zlonamjernih korisnika.
Nepriznavanje	Osiguravanje da se može dokazati da su dogovori postignuti zaista napravljeni.

Izvor: Cloud computing NCERT-PUBDOC-2010-03-293

U današnjem poslovanju neophodno je postaviti kvalitetan i pouzdan sustav upravljanja sigurnošću unutar poslovnih sustava te posebice upravljanjem sigurnošću informacijskih sustava kao njihovih vitalnih podsustava. Dobro planiranje, sustavne analize, procjene rizika, kontinuirano preispitivanje te evaluacije sigurnosnog stanja vrlo su bitne stavke sigurnosne razine poslovnog poduzeća. „Upravljanje sigurnosnim rizikom je trajan poslovni proces čiji je cilj osiguravanje pune dostupnosti informacijskog sustava. Smatra da se taj cilj ostvaruje kroz četiri osnovne funkcije upravljanja sigurnosnim rizikom:

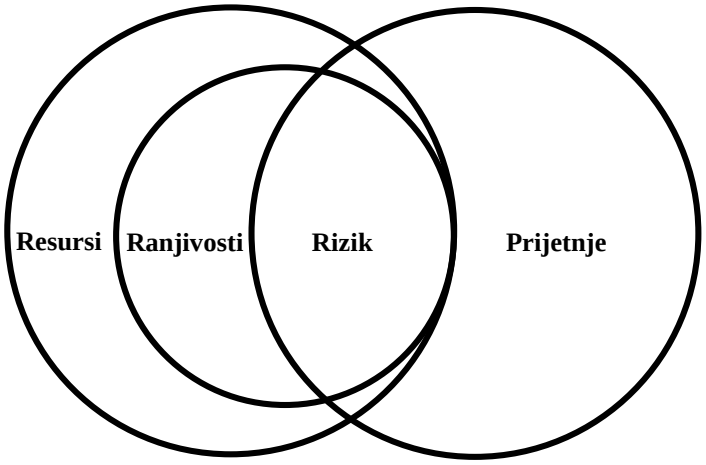
1. Utvrđivanje sigurnosne politike
2. Procjena sigurnosnog rizika
3. Umanjivanje sigurnosnog rizika
4. Evaluacija sigurnosnog rizika“ [4]

3.1. Sigurnosna politika

Sigurnosna politika je okvir za učinkovito i djelotvorno upravljanje sigurnošću poslovnih sustava. Ona bi se trebala formalizirati kroz odgovarajući dokument koji ne smije biti statičan zbog brzih promjena situacija na tržištu te pojavom novih oblika sigurnosnih prijetnji. Sigurnosna politika bi trebala biti skrojena za cijeli poslovni subjekt, ali također podijeljena po organizacijskim strukturama zbog različitih znanja i obaveza. Postoji krovna sigurnosna politika, opća organizacijska politika te funkcionalna politika te bi one trebale biti opisane standardima, procedurama i preporukama ponašanja za različite probleme.

3.2. Procjena i umanjivanje sigurnosnog rizika

Sigurnosni rizik se obično tretira kao funkcija tri varijable; informacijski resursi, prijetnje i ranjivosti. Varijable nisu nezavisne i postoji određena funkcijska povezanost među njima. Ukupni sigurnosni rizik je zbroj niza pojedinačnih rizika koji se ne mogu gledati kao cjelina jer se mjere umanjivanja rizika postavljaju za svaki rizik pojedinačno.



Slika 2: Sigurnosni rizik kao funkcija resursa, ranjivosti i prijetnji

Izvor: Garača, Željko (2009.): ERP sustavi

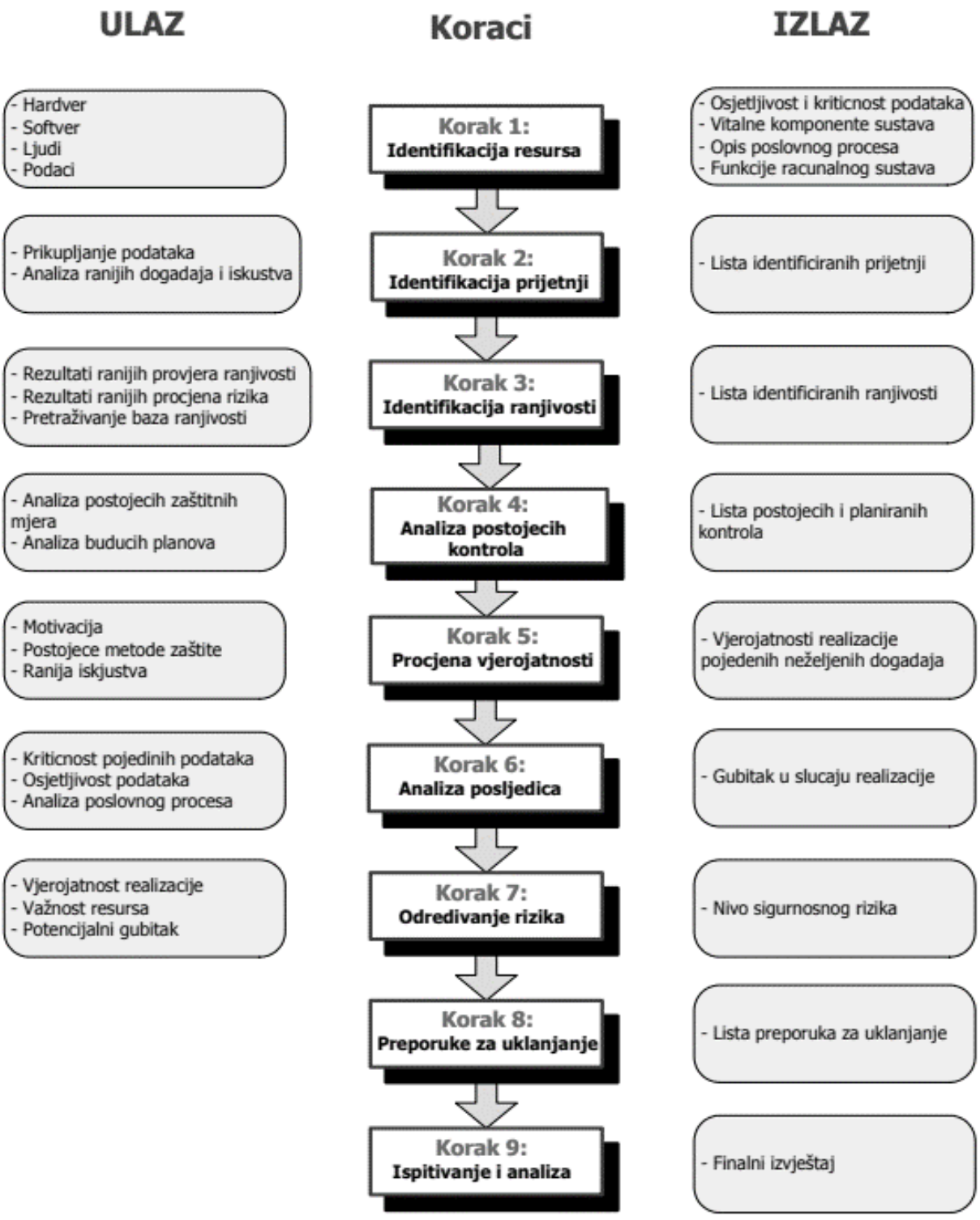
[4] Garača, Ž. (2009.): ERP sustavi, Sveučilište u Splitu Ekonomski fakultet, Split, str. 190.

Uzroci sigurnosnih rizika su prijetnje, odnosno pojave i postupci koji mogu djelovanjem izazvati neželjenje posljedice po informacijske sustave.

Procjena sigurnosnog rizika je vezana uz konkretno određivanje sigurnosnog rizika vezanog uz pojedini resurs. Postupci uključeni u ovaj proces su analiza svih prijetnji i ranjivosti, vjerojatnost realizacije sigurnosnih rizika i posljedice te cost benefit analiza sigurnosnih kontrola. Na temelju dobivenih rezultata menadžment odlučuje na kojim će se mjestima i u kojoj mjeri rizici reducirati.

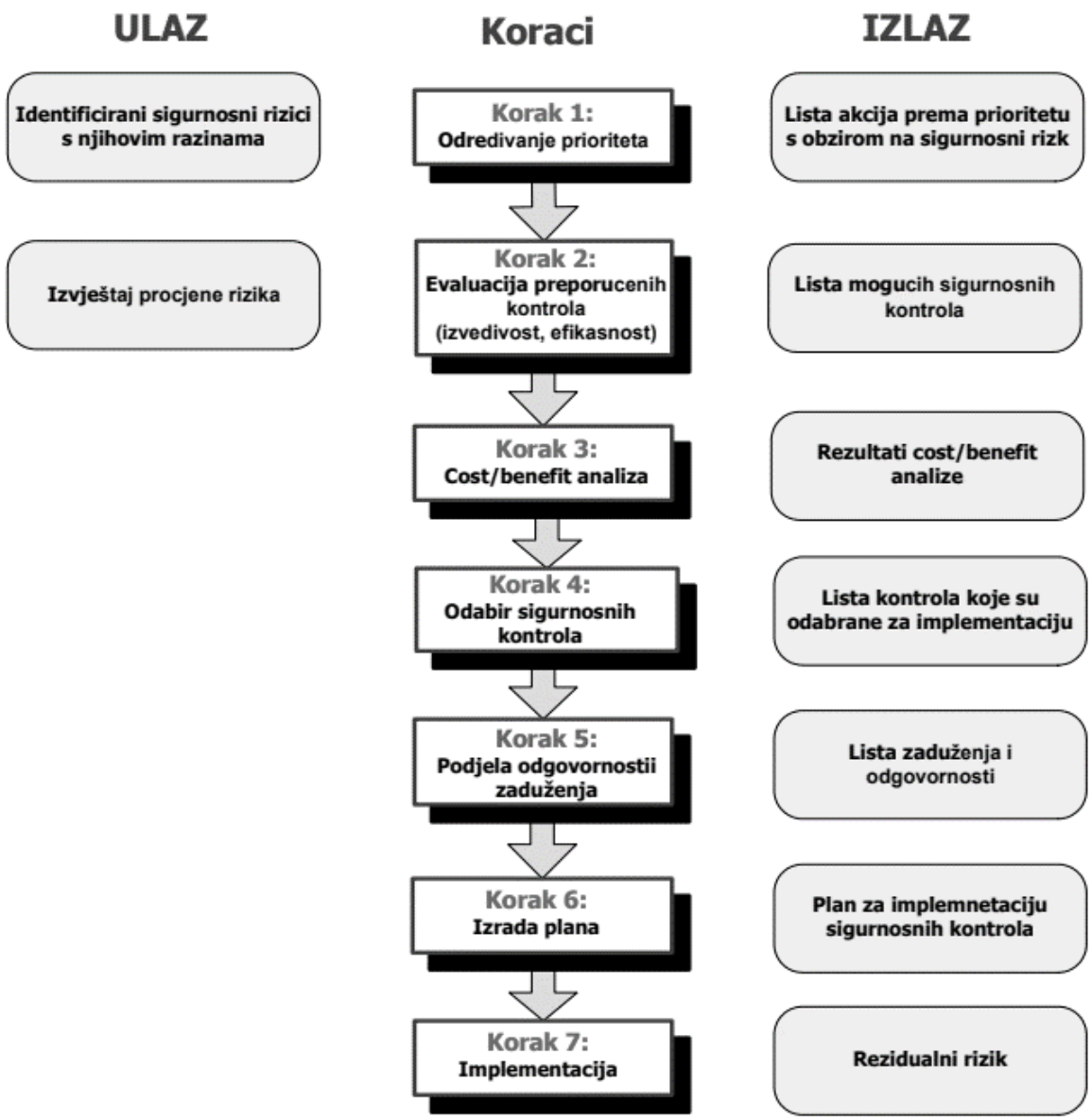
Umanjivanje sigurnosnog rizika je druga faza upravljanja sigurnosnim rizikom. U ovoj se fazi analiziraju, evaluiraju i implementiraju odgovarajući sigurnosni koraci. Sigurnosni rizik se umanjuje u onoj mjeri koja će zadovoljiti potrebe i ciljeve organizacije. Četiri pristupa umanjivanju sigurnosnih rizika su:

1. Umanjivanje rizika – pristup koji podrazumijeva izgradnju i provođenje određenih zaštitinih mehanizama koji smanjuju ranjivosti informacijskih resursa jer se na vjerojatnost pojedinih prijetnji ne može utjecati
2. Transfer rizika – pristup pri kome se rizik prenosi na nekog drugog uz odgovarajuću naknadu. Osim osiguranja moguć je i prijenos rizika na specijaliziranu organizaciju koja aktivnom primjenom mjera pridonosi umanjivanju rizika.
3. Prihvaćanje rizika – pristup pri kome se procijenjeni rizici prihvaćaju bez poduzimnja mjera umanjivanja ili transfera rizika. Pomoću cost benefit analize odlučuje se je li isplativo djelovati sigurnosim mehanizmima.
4. Odbacivanje rizika – pristup koji u potpunosti zanemaruje sigurnosne rizike



Slika 3: Procjena rizika

Izvor: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf



Slika 4: Proces umanjivanja rizika

Izvor: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf

Analiza sigurnosnih aspekata računovodstva u oblaku jedna je od bitnijih stavki kad govorimo o sigurnosti poslovnog subjekta. Njoj se mora pristupiti kao i analizi bilo kojeg drugog aspekta u poslovnom subjektu. Vrlo je bitno kreirati i primjeniti politiku sigurnosti i zaštitu povjerljivih podataka. To nije samo stvar tehnologije nego i stvar općenitog poslovanja, odnosno postavljanja politike, standarda, smjernica i procedura kojih se poslovni subjekt mora pridržavati. Prevencija je uvijek bolja od terapije i zato je važno primjeniti gore navedene mjere. Odgovornost za sigurnost poslovnog subjekta jednako je u rukama korisnika kao i pružatelja usluga. Edukacija je najvažniji dio jer su najčešće pogreške ljudske pogreške zbog neznanja i nepažnje.

4. SIGURNOSNE PRIJETNJE

Sigurnosne rizike računovodstvenih informacijskih sustava uzrokuju prijetnje, odnosno sigurnosne prijetnje (eng. *threat agents*). „Pod sigurnosnim prijetnjama podrazumijevaju se sve one pojave i postupci koji mogu utjecajem ili djelovanjem na pojedine informacijske resurse izazvati neželjene posljedice po informacijske sustave, i sam poslovni sustav. Njihov utjecaj na informacijske rsurse može se manifestirati kroz narušenost integriteta, odnosno ispravnosti i smislenosti, dostupnosti ili povjerljivosti.

Nadalje, prema kriteriju izvora sigurnosne prijetnje mogu se podijeliti u dvije skupine: ciljane prijetnje i opće prijetnje.
Ciljane prijetnje, iskorištavajući propuste u sigurnosnim i zaštitnim mehanizmima informacijskih odnosno informatičkih sustava, imaju za cilj stjecanje materijalne dobiti ili nanošenje štete.
Opće prijetnje stvar su slučajnosti i one su nenamjerne i nepredvidljive.
Procjena sigurnosnih prijetnji započinje detektiranjem svih mogućih prijetnji pri čemu se uzimaju u obzir sve ranija iskustva vezana uz neželjene događaje, vrste incidenata, motive, načine, vrijeme i lokacije napada na sigurnost. Uz prethodne, potrebno je razmotriti i moguće prijetnje.“[5]

4.1. Ciljane prijetnje

Najčešće su najveći rizici uzrokovani ciljanim prijetnjama pa se njima treba pridati posebna pozornost. Neke od tih prijetnji su: povreda podataka, nedostatan identitet, vjerodostojnost i upravljanje pristupom, nesigurna sučelja i API-ji, gubitak podataka, ranjivost sustava, otmica računa, nedovoljna pažnja, zlouporaba i neželjena upotreba oblak usluga, uskraćivanje usluge.

4.1.1. Povreda podataka

Povreda podataka (eng. *Data Breaches*) je kada neovlašteni pojedinac oslobađa, pregledava, krade ili upotrebljava osjetljive, zaštićene ili povjerljive informacije. Ona se događa uslijed

[5] Garača, Ž. (2009.): ERP sustavi, Sveučilište u Splitu Ekonomski fakultet, Split, str. 197.

ljudske pogreške, ranjivosti aplikacije ili kao sam cilj napada. To uključuje sve informacije do kojih se došlo, a nisu bile namijenjene javnom iznošenju, a najčešće su to financijski, zdravstveni i osobni podaci za provođenje različitih lažnih aktivnosti. Pružatelj oblak usluga Po CSA (2016.) Dropbox je više puta potvrdio napade u kojima su procurili podaci više od 68 milijuna korisnika.

4.1.2. Nedostatan identitet, vjerodostojnost i upravljanje pristupom

Nedostatak stabilnih sustava upravljanja identitetom, neuspjeh korištenja autentikacije, slabe lozinke i nedostatak automatske rotacije kriptografskih ključeva, lozinki i certifikata omogućavaju povrede podataka i napade na iste.

4.1.3. Nesigurna sučelja i API-ji

Sigurnost i dostupnost oblak usluga ovisi o sigurnosti osnovnih aplikacijskih programskih sučelja (eng. application programming interface, API). Dotična sučelja moraju biti dizajnirana za zaštitu od slučajnih i zlonamjernih pokušaja krađe putem provjere autentičnosti i kontrole pristupa, putem enkripcije i praćenja aktivnosti. Na primjeru Američke unutarnje prihodne usluge (eng. *US Internal Revenue Service*, IRS) koja je 2015. izložila preko 300 000 zapisa putem ranjivog API-ja vidi se javljanje rizika od izlaganja vrijednih podataka.

4.1.4. Gubitak podataka

Mogućnost trajnog gubitka podataka (eng. *data loss*) nije nužno iz zlonamjernih razloga. Ono može biti uzrokovano slučajnim brisanjem ili fizičkom katastrofom poput požara ili potresa, te može dovesti do trajnog gubitka podataka korisnika, osim ako pružatelj ili potrošač ne poduzmu odgovarajuće mjere za sigurnosno kopiranje informacija. Ako klijent šifrira svoje podatke prije nego što ih prenese u oblak, ali izgubi ključ za šifriranje, podaci će se izgubiti. „U oblaku raste prijetnja ugrožavanja podataka zbog mnoštva različitih međudjelovanja između rizika i izazova koji su jedinstveni oblak ili, još opasnije, zbog arhitekturalnih ili operacijskih svojstava oblaka.“[6]

[6] Carnet (2010.): Cloud computing [Internet], raspoloživo na:https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-03-293.pdf

4.1.5. Ranjivost sustava

Ranjivost sustava (eng. *System Vulnerabilities*) se može iskoristiti u programima koje napadači mogu koristiti za infiltriranje računalnog sustava u svrhu krađe podataka, preuzimanja kontrole nad sustavom ili ometanja servisnih operacija. Ranjivosti unutar komponenti operacijskog sustava stavljaju sigurnost svih usluga i podataka u značajni rizik.

4.1.6. Otmica računa

Metode napada poput krađe identiteta, prijevare i iskorištavanja softverskih ranjivosti i dalje postižu rezultate. Često su u upotrebi vjerodajnice i lozinke što povećava utjecaj takvih napada. Ako napadači dobiju pristup vjerodajnicama, oni mogu prisluškivati aktivnosti i transakcije određenih stranki, manipulirati podacima, vratiti krivotvorene informacije i preusmjeriti svoje klijente na nelegitimne web stranice.

4.1.7. Nedovoljna pažnja

Kreirajući poslovne strategije, rukovoditelji moraju razmotriti tehnologije oblaka i pružatelje oblak usluga. Ono neophodno za uspjeh je razvijanje dobrih smjernica i kontrolne liste za dubinsku procjenu prilikom ocjenjivanja tehnologija i pružatelja oblak usluga. Ona organizacija koja koristi oblak usluge bez prethodnih početnih koraka izlaže se brojnim komercijalnim, financijskim, tehničkim, pravnim i usklađenim rizicima koji ugrožavaju njegov uspjeh. 2012. godine javni oblak Amazon web servisa (AWS), koji se oslanja na Netflix, iskusio je prekid u regiji SAD-a zbog slučajnog brisanja podataka koji kontroliraju balansiranje opterećenja.

4.1.8. Zlouporaba i neželjena upotreba oblak usluga

Loše osigurana implementacija oblak usluge, besplatne probne usluge u oblaku i lažne prijave računa putem prijevare otkrivaju zlonamjerne napade. Primjeri zloupotrebe resursa temeljenih na uslugama u oblaku uključuju pokretanje DdoS napda, e-mail spama i pshishing kampanje, i sl. Kako bi se riješili zloupotrebe resursa, pružatelji oblak usluga moraju imati okvir odgovora na incident kao i opciju kojom korisnici mogu prijaviti zloupotrebu. Amazonov Elastic Cloud

Computing patio je od vrlo sofisticiranog napada skupine nepoznatih hakera koji su pronašli način za preokretanje koncepta kodova i stvorili lako dostupan ulaz za sebe u Amazonovu banku raspoložive procesorske snage.

4.1.9. Uskraćivanje usluge

Napadi uskraćivanjem usluga (eng. *Denial-of-service*, DoS) su napadi kojima se onemogućava korisnicima pristupiti njihovim podacima ili njihovim aplikacijama. Asimetrični DoS napadi na razini aplikacije iskorištavaju ranjivosti na web poslužiteljima, bazama podataka ili drugim resursima u oblaku, čime zlonamjerni pojedinac može izdvojiti aplikaciju s jednim iznimno malim sadržajem napada. Drugi se napadi mogu usmjeriti na jednako ograničene resurse. Ekonomski DoS ugrožava novčani tijek tvrtke, koristeći dinamičnu prirodu u oblaku kako bi prevladao sposobnost plaćanja za pokretanje. Isto tako, ljudski kapital neke organizacije može se brzo vezati za pravni posao za birokratski DoS i ostaviti tvrtku jednako nesposobnu za pružanje usluge. Pružatelj oblak usluga, Rackspace, doživio je DoS napad na svoje usluge 2014. godine. U još jednom spektakularnom primjeru napada, Amazon EC2 suočio se s još jednim velikim DoS napadom. Ovi napadi doveli su do prekida rada, poslovnih gubitaka te dugoročnih i kratkoročnih učinaka na poslovne procese žrtava.

5. METODE ZAŠTITE

„Metode zaštite računovodstva u oblaku dijele se na:

1. Organizacijske mjere – opće mjere zaštite informacijskih resursa koje se ne bave specifičnostima zaštite sustava već osiguravaju okvir za provođenje specifičnih mjera
2. Fizičke mjere – odnose se na onemogućavanje pristupa neovlaštenim osobama, uzimaju u obzir sve pristupne putove informacijskim resursima
3. Programske mjere – specifične za sigurnosne rizike informacijskih sustava, odnose se na podatke te se provode pomoću softvera i odnose se na sam softver“ [7]

Pobliže će se opisati svaka od mjera zaštite.

5.1. Organizacijske mjere

Organizacijske mjere su one mjere koje poduzima sam poslovni sustav s ciljem osiguranja željene razine funkcionalnosti sustava te integriteta podataka u uvjetima djelovanja pretpostavljenih oblika prijetnji. Organizacijskim mjerama smatra se sveukupni sadržaj mjera i postupaka iz oblasti sigurnosti, izrada potrebne dokumentacije koja je potrebna za njihovu primjenu te donošenje i izrada organizacijskih uputa kojima se one provode na radnom mjestu (Šehanović, Hutinski, Žugaj 2002).

Organizacijske mjere dijelimo na tri razine: infrastruktura informacijske sigurnosti, sigurnost pristupa treće osobe te outsorcing. Cilj infrastrukture informacijske sigurnosti je upravljati informacijskom sigurnošću unutar organizacije. Kako bi organizacija funkcionirala te da bi se štitile povjerljive informacije potrebno je poticati multidisciplinarni pristup sigurnosti informacija pravilnom suradnjom od najviših predstavnika u hijerarhiji organizacije do najnižih koji se koriste određenim informacijama.

Infrastruktura informacijske sigurnosti može se podijeliti na:

1. Tim za upravljanje informacijskom sigurnošću
2. Koordinacija rada informacijske sigurnosti

[7] Garača, Ž. (2009.): ERP sustavi, Sveučilište u Splitu Ekonomski fakultet, Split, str. 200.

3. Dodjela odgovornosti za informacijsku sigurnost
4. Proces autorizacije organizacijskih cjelina koje sudjeluju u obradi
5. Savjeti specijalista o informacijskoj sigurnosti
6. Suradnja između organizacija
7. Neovisni pregledi efikasnosti informacijske sigurnosti

Poslovna odgovornost managerskog tima je brinuti za informacijsku sigurnost. Vrlo je bitna koordinacija u većim poslovnim subjektima gdje se dogovaraju specifične uloge i odgovornosti. Politika informacijske sigurnost treba pružiti općenito vodstvo za dodjelu sigurnosnih uloga i odgovornosti u organizaciji. Gavni cilj jest da su sve odgovornosti informacijske sigurnosti jasno određene te da se točno znaju odgovornosti korisnika. Iz tog razloga najveća pažnja se usmjerava na identifikaciju i jasno definiranje dijelova imovine te sigurnosnih procesa pridruženih svakom pojedinom sustavu. U konačnici je potrebno dokumentirati te definirati razine ovlasti.
Kod sigurnosti pristupa treće zainteresirane strane razlikujemo dvije vrste pristupa. Fizičkim pristupom omogućava se trećim stranama pristup prostorijama s računalnom opremom i ormarima za pohranu, dok se logički pristup odnosi na pristup bazama podataka štićene organizacije te informacijskim sustavima.
Outsourcing je korištenje vanjskih poduzeća i pojedinaca za obavljanje pojedinog posla. Cilj poslovnog subjekta održati sigurnost informacija kada su one povjerene nekoj drugoj organizaciji. Kada se ugovara posao outsourcing-a bitno je kao i s ostalim trećim stranama sklopiti neku vrstu ugovora kojim se kontrolni mehanizmi, procjena rizika i sigurnosni postupcim provode kako bi se spriječilo neovlašteno korištenje informacija u organizaciji. Ugovorom o outsourcing-u zadani su određeni uvjeti odnosno zahtjevi kojih se treba držati prilikom obavljanja određenog posla za organizaciju. Glavna prednost outsourcinga je da se organizacija može usredotočiti na svoju osnovnu aktivnost dok i razvoj poslovnih procesa, jer su sporedni poslovi dani drugoj organizaciji koja obavlja to za njih. Nedostatci tog oblika su sigurnosni te je potrebna visoka razina kontrole i zaštite informacijskih sustava.

5.2. Fizičke mjere

Fizičke mjere zaštite se koriste kako bi se očuvala sigurnost informacijskih sustava. Fizička sigurnost ugrožava se u slučajevima elementarnih nepogoda, poplave, potresa i požara te ljudskih ranjivosti, kao što je sabotaža, krađa i neposlušnost. Primjena fizičke sigurnosti podrazumijeva proces upotrebe mjera zaštite kako bi se spriječio neovlašten pristup, oštećenje ili uništenje dobara. Cilj fizičke sigurnosti je spriječiti neautorizirane pristupe računalnom sustavu, zaštititi integritet podataka koji se pohranjuju na računalo, u slučaju raznih nepogoda spriječiti oštećenje ili gubitak podataka te spriječiti krađu podataka s računalnih sustava. Fizičke prijetnje se mogu podijeliti na dvije kategorije; prirodne nepogode te ljudski utjecaj.

Prirodne nepogode su takve prijetnje na koje čovjek ne može utjecati. Djelimo ih na:

1. Meteorološke nepogode
2. Geofizičke nepogode
3. Sezonski fenomeni
4. Astrofizički fenomeni
5. Biološke snage

Ljudske prijetnje su one prijetnje do kojih dolazi namjernim ili slučajnim potezima korisnika. Dijele se na:

1. Neposlušnost
2. Otkrivanje osjetljivih podataka
3. Sabotaža
4. Nenamjerno oštećenje imovine
5. Zlouporaba ovlasti
6. Neovlašten pristup podacima ili imovini
7. Krađa

Kod fizičke zaštite potrebno je štititi ne samo pojedino mjesto na kojem se povjerljive informacije nalaze, već i cijelu okolinu kako bi što teže bilo doprijeti do određenih informacija. U tu svrhu postoji zaštita okoline, zaštita prostorija, zaštita same opreme zatim kontrola pristupa.

Zaštita okoline obuhvaća zaštitu određenog prostora gdje se informacija nalazi. Takva zaštita postiže se postavljanjem kamera te postavljanjem zaštitara na određena mjesta.
Zaštita prostorija je usko vezana uz zaštitu okoline te se najčešće zaštićuje kamerama i alarmima te općenito implementacijom sustava protiv neovlaštenog ulaska u određenu prostoriju.
Zaštita opreme smatra se najvažnijim aspektom fizičke zaštite informacijskog sustava. Svaka oprema odnosno uređaj vrednuje se po svojim karakteristikama i namjeni stoga je razina zaštite različita za različiti uređaj ili opremu. Većinom ta zaštita podrazumijeva samo zaštitu primjerice osobnog računala na kojem zaposlenik radi ili zaštitu poslužitelja no potrebno je obratiti pažnju i na ostalu opremu. To se može postići stavljanjem prijenosnih medija s informacijama na sigurno mjesto, uništavanje starih medija na pravilan i siguran način, zaključavanje uređaja i sl.
Kontrola pristupa važna je kada je riječ o fizičkoj zaštiti informacija. Nju karakterizira potreba odobrenja za ulazak u objekt. Najčešće se primjenjuje kontrola pristupa na način da se zaposle zaštitari ili druge osobe koje će kontrolirati tko ima pristup. Osim tog načina kontrola pristupa provodi se putem mehaničkih sredstva i tehničkih sredstva. Kontrola pristupa nije ista za zaposlenike i korisnike u organizaciji, a razlikuje se u ovlastima. Najčešće se na ulazu u objekt identificiraju posjetitelji kako bi se umanjila mogućnost zlouporabe pristupa unutrašnjosti objekta ili nekim dijelovima informacijskih sustava. Postoje mnogi načini na koje se kontrola pristupa provodi a u današnje doba to su pametne kartice za kontrolu pristupa, skeniranje otiska prsta, šarenice oka ili pak prepoznavanje glasa.

5.3. Programske mjere

Programske mjere se mogu podijeliti na dvije razine: razina operacijskog sustava i razina korisničkih programa. U organizacijama se najčešće koriste višekorisnički operacijski sustavi te je za svakog korisnika potrebno odrediti područje dozvoljenog djelovanja i razinu pristupa informacijama što se čini zaštitom pomoću lozinki.

Zaštita na razini operacijskog sustava uključuje višekorisnički rad na računalu. Kako bi se zaštitile informacije ovlaštenim informacijama potpuni pristup ima samo administrator, a korisnik ima pristup samo onim informacijama koje mu omogući administrator sukladno korisnikovim ovlastima. U svrhu očuvanja sigurnosti informacija administrator svakom

korisniku određuje njegovo korisničko ime te lozinku kojima se koristi kako bi bez problema imao pristup relevantnim informacijama i kako bi obavljao zadatke za koje je zadužen. Sukladno obujmu posla i zadacima za koje je zadužen svaki korisnik zasebno dobiva određenu razinu ovlasti. Svako računalo može imati više administratora te više korisnika, a svi suvremeni operacijski sustavi poput Windows-a, MacOs-a, Linux-a i Unix-a omogućuju upravo ovakvu razinu zaštite.

Zaštita na razini korisničkih programa drugi je korak u sigurnosti informacija. U informacijskom sustavu koristi se određeni korisnički program putem kojega se obavljaju zadaci i aktivnosti vezani uz određenu obavezu prema organizaciji. Korisnički programi štite se kroz tri razine. Prva razina odnosi se isključivo na čitanje podataka iz baze, druga razina omogućuje unos i promijenu podataka u bazi, a treća razina uz sve to omogućuje i brisanje podataka. Kako bi se osigurala informacijska sigurnost brisani podaci ne uklanjaju se na direktan način već se pohranjuju u datoteke kojima ima pristup jedino administrator. Administrator zatim provjerava podatke i odlučuje da li će se oni uistinu izbrisati ili ne.

5.4. Primjeri metoda zaštite na ciljane prijetnje

5.4.1. Nedostatan identitet, vjerodostojnost i upravljanje pristupom

Potrebno je:

1. provoditi strogi nadzor nad lancem nabave i provoditi cjelokupne procjene isporučitelja
2. odrediti zahtjeve za ljudskim resursima kao dio pravnog ugovora
3. zahtijevati transparentnost u informacijskoj sigurnosti i praksi upravljanja, kao i usklađenost izvještavanja
4. odrediti proces obavještavanja o sigurnosnim problemima

5.4.2. Nesigurna sučelja i API-ji

Potrebno je:

1. analizirati sigurnosne modele sučelja davatelja cloud computing usluga
2. prenositi šifrirani signal i osigurati odgovarajuću autentikaciju i provjeru pristupa

3. razumjeti da se preko sučelja povezuju na druge sustave koji mogu biti sigurnosno ugroženi (pa se tako mogu neplanirano i neoprezno i sami izložiti riziku)

5.4.3. Gubitak podataka

Potrebno je:

1. implementirati sučelje s dobrom kontrolom pristupa
2. kriptirati podatke i zaštiti njihov integritet podataka
3. analizirati zaštitu podataka za vrijeme dizajna i izvođenja te
4. nakon što korisnici oduče za prestanak korištenja poslužitelja, davatelji usluga bi trebali trajno ukloniti korisničke podatke sa poslužitelja; korisnici bi trebali sklopiti ugovor s davateljima usluge koji sadrži detalje oko postojanja sigurnosnih mjera i strategije pridržavanja.

5.4.4. Otmica računa

Potrebno je:

1. zabraniti dijeljenje pristupnih vjerodajnica između korisnika i poslužitelja
2. gdje god je moguće koristiti snažne dvofaktorske autentikacijske tehnike
3. izvoditi proaktivno praćenje za otkrivanje neovlaštenih aktivnosti
4. razumijevati sigurnosne politike i SLA (eng. service level agreement) davatelja cloud computing usluga

5.4.5. Zloupotreba i neželjena upotreba oblak usluga

Potrebno je:

1. uvesti složeniju početnu registraciju i provjeru procesa
2. poboljšati praćenje i koordinaciju prijevara koje se izvode preko kreditnih kartica
3. uvesti cjelokupno provjeravanje mrežnog prometa korisnika
4. ugraditi nadzor javnih crnih lista na kojima su navedeni zlonamjerni korisnici (tj. adrese s kojih se korisnici prijavljuju) kako bi se zaštitili vlastiti sustavi

6. ZAKLJUČAK

Zaključak koji se može donijeti na temelju ovoga rada je nezaobilaznost sigurnosnoga aspekta u računalstvu, a tako i u računovodstvu u e-oblaku. Uslijed razvoja tehnologije računovodstvo se kao disciplina usporedno razvijalo i dalje se razvija te je neizostavni dio istoga postala informatička tehnologija. Zbog neznanja i osjećaja (ne)sigurnosti većina poslovnih organizacija i dalje koristi tradicionalno računovodstvo, odnosno ne povezuje podatke i financijske transakcije putem interneta već se isključivo koristi svojim lokalnim računalima. Računovodstvo u e-oblaku definitivno predstavlja budućnost računovodstvenih informacijskih sustava zbog nižih troškova ulaganja i održavanja, pristupačnosti i fleksibilnosti sustava, brzine i načina obrade podataka, usklađenosti sustava, jednostavnosti i efikasnosti i smanjenja rizika od uništenja podataka. Negativni aspekt korištenja informacijskog sustava u oblaku je sigurnosni rizik, ali upravo na temelju napada postoji prostor za razvitak i napredak discipline i samih sustava kojima se ista koristi. Prepreke razvitku su nedovoljno poznavanje tehnologije, previsoka cijena usluge, pravna i zakonska nesigurnost, nesigurnost fizičke lokacije podataka i sigurnosni rizik. Na kraju je moguće zaključiti kako se budući razvoj računovodstvenih informacijskih sustava u e-oblaku može ostvariti i ubrzati edukacijom uopće i educiranjem konkretnih poslovnih organizacija i računovođa.

LITERATURA

1. Crnković, L., Hadrović Zekić, B., Mijoč, I. (2006.): Povijesni razvoj računovodstvenog informacijskog sustava – od glinene pločice do računala
2. Garača, Ž. (2008.): Poslovni informacijski sustavi
3. Garača, Ž. (2009.): Erp sustavi
4. Lukić, K. (2016.): Računovodstvo u oblaku u Republici Hrvatskoj, završni rad
5. Novak, A., Zvonar, B., (2015.): Primjena računovodstvenih programa u oblaku [Internet], raspoloživo na: https://www.bib.irb.hr/785172
6. Spremić, I. (2003.): Računovodstvo
7. Stipić, A., Bronzin, T. (2011.): Mobilni BI: Prošlost, sadašnjost i budućnost
8. Zovko, I. (2017.): Sigurnost i računarstvo u oblaku [Internet], raspoloživo na: http://darhiv.ffzg.unizg.hr/id/eprint/8968/1/Sigurnost%20i%20racunarstvo%20u%20oblaku.pdf
9. Carnet (2010.): Cloud computing [Internet], raspoloživo na:https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-03-293.pdf
10. Carnet (2003.) : Upravljanje sigurnosnim rizicima [Internet], raspoloživo na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf
11. Noobpreneur (2016.): How safe is cloud accounting? [Internet], raspoloživo na: https://www.noobpreneur.com/2016/11/23/cloud-accounting-safety/

PRILOZI

SLIKE:

Slika 1: Povezanost računovodstvenog podsustava i upravljanja
Slika 2: Sigurnosni rizik kao funkcija resursa, ranjivosti i prijetnji
Slika 3: Procjena rizika
Slika 4: Proces umanjivanja rizika

TABLICE:

Tablica 1: Uobičajeni zahtjevi sigurnosti

GRAFIKONI:

Grafikon 1: Zapreke u korištenju koncepta računalskog oblaka u Republici Hrvatskoj

SAŽETAK

Ključne riječi: računovodstvo u oblaku, sigurnosne prijetnje, metode zaštite

Suvremena tehnologija omogućava nam novi pogled na aktivnosti i podaktivnosti poslovnog poduzeća. Nužno je da se poslovni subjekt prilagodi i da prihvati razvoj tehnologije te je implementira u svoje poduzeće. Ovaj rad bazira se na računovodstvu u oblaku kao relativno novom vidu poslovno informacijskih sustava te njegovim sigurnosnim aspektima. Računovodstvo je disciplina koja se bavi evidencijom i analizom poslovnih procesa u poslovnom poduzeću. Računovodstveni informacijski sustav (RIS) označava podsustav ukupnog informacijskog sustava koji je temeljni izvor informacija o poslovanju poduzeća. Korištenje računovodstvenog informacijskog sustava uvelike je olakšalo poslovanje kako zbog lakšeg pristupa informacijama tako i zbog postojanja mogućnosti analize podataka nužne za daljne poslovno odlučivanje. Kada govorimo o računovodstvu u oblaku možemo ga definirati kao vođenje računovodstva preko interneta kroz najam softvera, servera i druge informatičke opreme od nekog drugog poslovnog subjekta. Njegove glavne prednosti u odnosu na tradicionalni pristup su niži troškovi ulaganja i održavanja, pristupačnost i fleksibilnost sustava, brzina i način obrade podataka, usklađenost sustava, jednostavnost i efikasnost i smanjenje rizika od uništenja podataka. Glavni nedostatak računovodstva u oblaku je sigurnosni rizik, odnosno rizik od gubljenja povjerljivih informacija. Upravljanje sigurnosnim rizicima zahtjevan je i složen posao i mora biti odrađen profesionalno. U upravljanje sigurnosnim rizicima uvrštavamo aktivnosti utvrđivanja sigurnosne politike, procjenu sigurnosnog rizika, umanjivanje sigurnosnog rizika te evaluaciju sigurnosnog rizika. Sigurnosne prijetnje definiramo kao pojave koje mogu utjecajem i djelovanjem na pojedine informacijske resurse izazvati neželjene posljedice po informacijske sustave kao i na sam poslovni sustav. Zbog toga je potrebno izraditi i implementirati mjere zaštite, odnosno procedure koje umanjuju sigurnosne rizike. Njih možemo podijeliti na organizacijske, fizičke i programske mjere. Odgovornost za sigurnost poslovnog subjekta jednako je u rukama korisnika kao i pružatelja usluga. Edukacija je najvažniji dio jer su najčešće pogreške ljudske pogreške zbog neznanja i nepažnje.

SUMMARY

Key words: cloud accouting, safety threats, protection methods

Contemporary technology allows us a new look at the activities and sub-activities of a business enterprise. It is essential that a business entity adjusts and accepts the development of technology and implements it into its enterprise. This paper is based on cloud accounting as a relatively new form of business information systems and its security aspects. Accounting is a discipline that deals with the records and analysis of business processes in a business enterprise. The Accounting Information System (AIS) is the subsystem of the overall information system, which is the basic source of information on the business of the enterprise. The use of accounting information systems greatly facilitated business operations due to easier access to information as well as the ability to analyze data necessary for further business decision making. When we talk about cloud accounting we can define it as keeping accounting over the Internet through leasing software, servers, and other IT equipment from another business entity. Its main advantages over the traditional approach are lower investment and maintenance costs, system availability and flexibility, speed and data processing, system compliance, ease and efficiency, and reduction of data destruction risks. The main disadvantage of cloud computing is the security risk and the risk of losing confidential information. Managing security risks requires complex work and needs to be done professionally. In the management of security risks, we include the activities of choosing the security policy, assessing the security risk, reducing the security risk and evaluating the security risk. Security threats are defined as phenomena that may have an adverse effect on the information systems as well as the business system itself by influencing and acting on certain information resources. Therefore, it is necessary to develop and implement protection measures and procedures that reduce the security risks. We can divide them into organizational, physical and program measures. Responsibility for the security of a business entity is the same in the hands of users as well as service providers. Education is the most important part because the most common mistakes of human error are ignorance and neglect.